**Christopher J. Schatz, OSB No. 915097**
**Assistant Federal Public Defender**
**101 SW Main Street, Suite 1700**
**Portland, OR 97204**
**Tel: (503) 326-2123**
**Fax: (503) 326-5524**
**Email: chris_schatz@fd.org**

**Ruben L. Iñiguez, OSB No.**
**Assistant Federal Public Defender**
**101 SW Main Street, Suite 1700**
**Portland, OR 97204**
**Tel: (503) 326-2123**
**Fax: (503) 326-5524**
**Email: ruben_iniguez@fd.org**

**Attorneys for Hock Chee Khoo**

**IN THE UNITED STATES DISTRICT COURT**

**FOR THE DISTRICT OF OREGON**

**PORTLAND DIVISION**

| | |
|---|---|
| **UNITED STATES OF AMERICA,**<br><br>**Plaintiff,**<br><br>**vs.**<br><br>**HOCK CHEE KHOO, et al.,**<br><br>**Defendants.** | **CR 09-321-KI**<br><br>**MEMORANDUM OF POINTS AND AUTHORITIES IN SUPPORT OF MOTION TO EXCLUDE IMAGES OF THE WU LAPTOP AND EXTERNAL HARD DRIVE.** |

**TABLE OF CONTENTS**

**PAGE**

## TABLE OF AUTHORITIES

### FEDERAL CASES

**FEDERAL STATUTES AND RULES**

**MISCELLANEOUS**

## INTRODUCTORY STATEMENT

For the reasons hereinafter set forth, Mr. Khoo moves this Court to exclude from evidence certain digital images of the Wu Laptop hard drive and an external hard drive device used by Mark Hansen, on October 17, 2006, to make a backup copy of the laptop hard drive. Mr. Khoo's Motion to Exclude Images of the Wu Laptop and External Hard Drive, filed concurrently herewith, challenges the admissibility of these "copies" or digital images of Shengbao "Jesse" Wu's laptop hard drive (hereinafter referred to as the "Wu Laptop").

Mr. Khoo's motion asserts two evidentiary bases for exclusion. First, that the circumstances surrounding the creation of these images by Special Agent Joel Brillhart of the Federal Bureau of Investigation (FBI), and by Mark Hansen, are so dubious as to deprive these copies of the degree of trustworthiness requisite to treating them as being what the government has represented them to be - forensically identical copies of the data content and configuration of the Wu Laptop as of October 17, 2006. Thus, Federal Rule of Evidence 901 precludes admission of the forensic images. Second, a genuine question presently exists as to the evidentiary integrity of the original Wu Laptop hard drive at the time it was initially imaged by Hansen on October 17, 2006, and at the time it was turned over to the FBI on October 20, 2006. Mr. Khoo's forensic expert Michael Bean has identified a number of fundamental and troubling deficiencies in the manner in which the Acronis and Laptop images were created. *See* Declaration Of Computer Forensics Expert Michael A Bean In Support Of Motion To Exclude Images Of The Wu Laptop And External Hard Drive (hereinafter "Declaration of Forensic Computer Expert Bean"), dated May 27, 2010, at pp. 3-8. Discrepancies have also been discovered as between the content of the Acronis and Laptop images. Accordingly,

even if these copies qualify as "duplicates," their admissibility is in question because they cannot satisfy the best evidence rule as codified in Rules 1002 and 1003 of the Federal Rules of Evidence.

Resolution of these foundational evidentiary issues is appropriate at this time because the charges raised in the indictment are predicated on the data content and configuration of the Wu Laptop computer as it purportedly existed prior to October 17, 2006. Should the government not be in a position to establish to this Court's satisfaction that the Acronis and/or Laptop images constitute trustworthy evidence, the charges against defendants will necessarily fail. Given that resolution of the forensic issues pertaining to the admissibility of the Acronis and Laptop images is likely to be favorable to Mr. Khoo, thereby relieving him from the personal turmoil and expense of being a defendant in a federal criminal case, due process calls for as early an adjudication of said issues as possible.[1] Early resolution is also appropriate given this Court's gate keeping function with respect to novel forms of evidence of uncertain reliability. *See Kumho Tire v. Carmichael*, 526 U.S. 137, 153-56 (1999)(applying *Daubert* criteria and analysis to tire examiner's forensic methodology).

## STATEMENT OF THE CASE

Mr. Khoo is currently charged with one count of conspiracy in violation of 18 U.S.C. §371 (alleging Intent to Commit Wire Fraud, 18 U.S.C. §1343, Theft of Trade Secrets, 18 U.S.C. §1832, and Fraud in Connection with Computers, 18 U.S.C. §1030(a)(4)), and three substantive counts of wire fraud in violation of 18 U.S.C. §1343. Trial is scheduled to commence March 8, 2011.

[1]Federal Rule of Evidence 104(c) provides that hearings on preliminary matters involving the admission of evidence "shall be so conducted when the interests of justice require."

## STATEMENT OF FACT

### A. Hoffman's Discovery Of Purported Economic Espionage Activity And Seizure Of The Wu Computer.

In August of 2006, Lawrence "Drew" Hoffman, owner of several after-market auto parts manufacturing and distributing entities, including The Hoffman Group (THG), discovered an eBay auction site that appeared to be selling a type of automobile part generically known as the vertical door lift. The part offered for sale on the eBay site appeared to be almost identical to a similar part, the "130 Degree Lambo Vertical Door Kit," manufactured and distributed by Hoffman's companies. The auto part on the eBay site was being marketed under the brand name "Cleanline Motor Sports." Further research revealed that the "Cleanline Motor Sports" name had been registered by a company named "JES Suppliers, LLC."

Hoffman subsequently discovered that "JES Suppliers, LLC," had been incorporated in the State of Oregon on May 18, 2006, by Mssrs. Wu, Soutavong, and Khoo.[2] Soutavong was then a current employee of THG, in a technical sales support function. Wu was employed by The Hoffman Group – Hong Kong, Ltd., a wholly owned subsidiary of THG, located in China. Wu's function was to assist in the design and development of new products and oversee THG manufacturing activity in China. Khoo was a former employee of THG and another Hoffman company, "Marix." Khoo's employment functions had been confined to warehouse work and shipping.[3]

---

[2]In addition to initiating his own investigation into JES Suppliers, LLC, and the alleged theft of trade secrets, Hoffman also contacted the FBI on September 1, 2006.

[3]THG Confidentiality Agreements signed by Soutavong and Khoo have been released as discovery. No similar confidentiality agreement signed by Wu has been produced to date.

On October 17, 2006, Wu returned to the United States.[4] Wu had been summoned back to the United States by Hoffman, who met Wu at the airport. Upon his arrival at the THG office site, Hoffman convinced Wu to leave his laptop computer (a computer that was actually owned by THG) with Mark Hansen, who was introduced to Wu as a THG employee and computer consultant, so that it could be upgraded.

Hansen, a computer analyst employed by Northwest Countermeasures, had been hired by Hoffman to examine Wu's laptop. Hansen took custody of Wu's computer. After Wu went off with Hoffman, Hansen turned Wu's laptop computer on and then opened a folder marked "private." In this folder, Hansen purportedly found information pertaining to both THG and another entity, identified as "JES Suppliers, LLC." Hansen moved the "private" folder to the laptop desktop. Over an hour then elapsed during which it is impossible to determine what, if any, substantive changes were made by Hansen to the laptop's data content and configuration. Hansen then made a backup file of the laptop hard drive on an external USB hard drive device using Acronis software.

Hoffman took the Wu laptop computer home, turned it on again, and examined its contents. Hoffman made "screen shots" of a chat program contact list he found on the computer, which he saved to a subfolder in the "private" folder he named "QQ". Hoffman also tried to copy the contents of the "private" folder to a thumb drive, but was unable to do so.

According to Hoffman, the "private" folder contains THG proprietary information and trade secrets belonging to THG. In addition, Hoffman contends that the "private" folder also contains a Filemaker software database (a computer data management application known as "Platipus") that

---

[4] Although Wu is charged as the lead defendant, he has not made an appearance in this case and he is currently in China.

he had previously customized and developed for use by THG with respect to its after-market auto parts business.

On October 18, 2006, Wu and Soutavong were both terminated from employment at THG. On October 20, 2006, Hoffman brought the Wu Laptop to the FBI regional computer forensic laboratory, where he met with FBI Special Agent Phil Slinkard. In SA Slinkard's presence, Hoffman again turned on the laptop and proceeded to copy the "private" folder to an external Western Digital USB disk drive. Hoffman then turned the laptop over to SA Slinkard and as well the USB hard drive used by Hansen (containing the Acronis backup file). Using Forensic Tool Kit software, an image of the laptop as of October 20, 2006, was made (hereinafter the "Laptop image") by FBI Special Agent Joel D. Brillhart.[5] An image of the USB hard drive was also made at this time by Special Agent Joel Brillhart. This USB hard drive image containing the Acronis backup file is referred to herein as "the Acronis image." It is these images – the Acronis and Laptop images – that are the subject of Mr. Khoo's motion to exclude for inadequate authentication and violation of the best evidence rule.

## POINT I

## THE BASIC STANDARDS GOVERNING AUTHENTICATION OF COMPUTER–BASED EVIDENCE UNDER FRE 901.

Evidence may be admitted only if the court "is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims." F.R.E. 901(a). The key purpose of the authentication requirement is to ensure that only genuine and trustworthy evidence is

[5]The laptop and the USB hard drive device were subsequently returned to Hoffman by Special Agent George Chamberlain on November 20, 2006.

considered at trial. *See, e.g., United States v. Panero*, 266 F.3d 939, 951 (9th Cir. 2001) (for evidence to meet authenticity requirement, trial court must be satisfied that it is accurate, authentic, and generally trustworthy). This inquiry is a threshold to introduction of evidence, not simply a matter bearing on the weight to be afforded it. *See United States v. Logan*, 949 F.2d 1370, 1377-78 (5th Cir. 1991); *United States v. Stearns*, 550 F.2d 1167, 1170 (9th Cir. 1977) (before photograph can be admitted, it must be authenticated as technically accurate representation of scene photographed).

Accuracy concerns apply just as forcefully to computer–based evidence as they do to all other forms of evidence. *See Manual for Complex Litigation*, §11.447 (Federal Judicial Center 4th ed. 2004). In fact, they may apply even more forcefully because the widespread shift from written to digital records has exposed fundamental differences between how inaccuracies are detected in each medium. *Id*. ("Computerized data...raise unique issues concerning accuracy and authenticity."). As one commentator has explained, "the key to the inspection paradigm of traditional, physical records is that the ability to detect traces of change could be found from evidence in the record being inspected. Writing can be smeared or smudged, . . . [a] page can be torn out of a document, . . . [o]ne can sense a cut-and-paste job in a photograph." George L. Paul, *Foundations of Digital Evidence* at 21 (ABA 2008). On the other hand, "[n]early every application in use today provides the ability to modify existing content in such a way that modification would not be detectable unless a history of the change was being recorded....In short, almost everything that can be digitized can be modified, leaving no indication it has been changed." *Id*. at 22; *see also In re Vee Vinhnee*, 336 B.R. 437, 445, 2005 WL 3609376 at *5 (9th Cir. BAP (Cal.) 2005) ("digital technology makes it easier to alter text of documents that have been scanned into a database, thereby increasing the importance of audit procedures designed to assure the continuing integrity of the records."). The modern reality is that

"[n]o matter how carefully one studies things, one may only be able to discern the most recent version of a digital file, not its makeup seventeen versions ago much less its original composition." *Foundations of Digital Evidence*, *supra*, at 22; *see also* 2 Kenneth S. Broun et al., *McCormick on Evidence* at 24 n.16 (6th ed. 2006)("Not only are digital images easier to manipulate, meaning changing colors, moving images and other alterations, these manipulations are difficult to detect.").

Therefore, where there is a genuine concern that computer–based evidence may have been altered or manipulated, an additional degree of scrutiny by the courts is appropriate. *See* Saltzburg, Martin, and Capra, *Federal Rules of Evidence Manual* §901.02[3] (9th ed. 2006) ("[W]hen it comes to the question of whether the Judge must make a preliminary determination before admitting evidence, as opposed to simply deciding there is enough for the jury to decide whether to rely on the evidence, the best reading of Rule 901 would be to follow a case-by-case approach and to demand a more substantial foundation where the circumstances might create a suspicion that evidence is altered or fabricated."). In order to warrant this heightened scrutiny, the objecting party must make a showing sufficient to raise serious concerns about authenticity. Thus, the simple "fact that it is possible to alter data contained in a computer is plainly insufficient to establish untrustworthiness." *United States v. Bonallo*, 858 F.2d 1427, 1436 (9th Cir. 1988).

Although a hypothetical suggestion that tampering may be possible will not suffice to preclude admissibility, it would be similarly inappropriate to force the objecting party to present a *prima facie* showing that tampering in fact occurred. *See United States v. Jackson*, 208 F.3d 633, 638 (7th Cir. 2000) (even if web postings, in which white supremacists took responsibility for racist mailings, qualified for business records hearsay exception, they were "inadmissible if the source of information or the method or circumstances of preparation indicate a lack of trustworthiness;" thus,

proponent failed to authenticate web postings, since there was some evidence that she had the motive and technological ability to place them on the groups' web sites herself).[6] Instead, if serious concerns are raised as to the source of the evidence in question, and those concerns are based in evidence, district courts should feel compelled to take a "hard look" at the authentication requirements. *Id.*; *see also Federal Rules of Evidence Manual, supra*, at § 901.02[3]; *2 McCormick on Evidence*, *supra*, at 24 ("[W]hen there is a significant risk of tampering such as now exists with digital images, the court could require a more complete foundation.").[7]

## POINT II

## THE LAPTOP IMAGE AND THE ACRONIS IMAGE SHOULD BE EXCLUDED FROM EVIDENCE DUE TO LACK OF ADEQUATE AUTHENTICITY UNDER RULE 901.

Three key issues have arisen with respect to the FBI's Wu Laptop image that implicate Rule 901's authentication requirement - i.e. the provision of evidence "sufficient to support a finding that the matter in question is what its proponent claims." Two of these issues also implicate Hansen's Acronis image. First, the motive, opportunity, and ability of Hansen and Hoffman to alter the information on Wu's computer pose a significant risk of impropriety that warrants rigorous

---

[6]In *Perfect 10, Inc. v. Cybernet Ventures, Inc.*, 213 F. Supp. 2d 1146, 1153-54 (C.D. Cal. 2002), *Jackson* was acknowledged in principal but distinguished as applied to the facts of that particular case.

[7]This heightened concern with the source of evidence finds support in Ninth Circuit case law, where courts have stressed not only the government's burden to make a prima facie showing of authenticity, but also to establish a sufficient connection between the specific evidence being offered and the defendant. *See, e.g., United States v. Tank*, 200 F.3d 627, 630–31 (9th Cir. 2000); *United States v. Black*, 767 F.2d 1334, 1342 (9th Cir. 1985).

application of the threshold requirements of Rule 901. Second, the FBI and Hansen employed methods of forensic imaging that fall well below standard industry practices geared towards accuracy. Third, at least 1,000 additional images are present on the Laptop image of Wu's laptop computer hard drive that are not present in the same form in the Hansen Acronis image. These circumstances warrant exclusion of the Wu Laptop image and the Acronis image due to inadequate authentication under Rule 901.

**A. Hansen And Hoffman Possessed The Motive, Opportunity, And Ability To Alter The Contents Of The Wu Hard Drive, And The Data Reproduction Methods They Used Resulted In A Tainted Chain Of Custody Requiring Heightened Scrutiny Under Rule 901**.

In this case, the government can only connect the information on Wu's computer to Wu via third parties. Thus, this case does not present the simple scenario where the subject evidentiary materials were in the possession of the defendant upon confiscation by the government, *see Black*, 767 F.2d at 1342, or where the defendant admitted (and other witnesses corroborated) the defendant's association with the evidence in question. *See Tank*, 200 F.3d at 630–31 (sufficient authentication to introduce chat logs where defendant admits screen names associated with chat logs are his, and several witnesses corroborate this association). Instead, Wu was manipulated into turning over his computer to an adverse third party - Hoffman - a third party who subsequently initiated a civil lawsuit against Wu and the other defendants in the instant case, and who has sophisticated knowledge of computer technology. It is here, where the chain of custody between the defendant and the evidence in question is indisputably broken by an intervening third-party, that the Seventh Circuit's analysis in *Jackson* offers guidance.

At its core, *Jackson* stands for the proposition that where evidence is of a type that is easily open to alteration or manipulation, and the circumstances disclose a suspicious chain of custody and the possibility of data manipulation, courts should employ a higher degree of scrutiny. 208 F.3d at 638; *see also United States v. Clonts*, 966 F.2d 1366, 1368 (10th Cir. 1992) ("[I]f the evidence is open to alteration or tampering, or is not readily identifiable, the trial court requires a more elaborate chain of custody to establish that the evidence has not been tampered with or altered.")(citations omitted); *Federal Rules of Evidence Manual, supra,* at §901.02[3]. That is not to say that such scrutiny inevitably leads to exclusion of the evidence, *see Bonallo*, 858 F.2d at 1436, but where a third party had the motive, opportunity, and ability to tamper with evidence that is subsequently turned over to the government, concerns about its authenticity should be afforded great weight. *See, e.g., United States v. Safavian*, 435 F. Supp. 2d 36, 41 (D. D.C. 2006) (suggesting that exclusion of e-mail is appropriate where specific evidence of alteration is offered and a break in the chain of custody has occurred).

Such concerns form the very basis for the rule of authentication. *See 2 McCormick on Evidence*, *supra*, at 57 ("The principal justification urged for this judicial skepticism toward the recital of authorship in documents is that it constitutes a necessary check on the perpetration of fraud." Where Y is suing X on the basis of the contents of a tangible document, it is "possible that Y has fabricated the writing to provide herself with a cause of action."). These concerns permeate the present case, where Hansen and Hoffman were intervening parties accessing, handling, and creating images of the Wu computer. *See* Eoghan Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet* at 220 (2d ed. 2004) ("Ultimately, the trustworthiness of digital evidence comes down to the trustworthiness of the individual who collected it.").

**B. The FBI Failed To Follow Proper Forensic Protocol In Producing The Wu Laptop Image**.

Like any procedure striving for accurate and reliable results, forensic examination of digital evidence relies heavily on accountability and transparency through thorough documentation. *See Digital Evidence and Computer Crime*, *supra*, at 112 ("To provide a transparent view of the investigative process, final reports should contain important details from each step, including reference to protocols followed and methods used to seize, document, collect, preserve, recover, reconstruct, organize, and search key evidence."); *see also* U.S. Department of Justice, *Electronic Crime Scene Investigation: A Guide for First Responders* at 3 ("The examination process helps to make the evidence visible and explain its origin and significance....Examination notes must be preserved for discovery or testimony purposes. An examiner may need to testify about not only the conduct of the examination but also the validity of the procedure").

The standard forensic procedure governing documentation and duplication of computer-based information is relatively straightforward. Proper duplication of Hansen's Acronis backup file and the Wu Laptop hard drive would have occurred as follows:

1) The devices (the Wu laptop and the removable device provided by Hansen) would have been provided to the FBI;

2) The FBI (referring to a properly trained and certified forensic computer examiner) would have documented the make, model, and serial number of the hardware to be duplicated;

3) The FBI would have obtained and recorded any CMOS[8] or BIOS[9] setting for any device that had a CPU;

4) The hard drives would have been removed from the Wu laptop and the external hard drive removable device provided by Hansen;

5) The FBI would have documented the make, model, serial number and size of the hard drives;

6) The FBI would have connected the hard drives to hardware write blockers so that no changes could be made to the hard drives during the duplication process;

7) The FBI would document the type of hardware write blocker used;

8) The FBI would produce the forensic images of the hard drives using software specifically designed for this purpose;

9) The FBI would document the software and hardware used to create the forensic images.

*See* Declaration of Forensic Computer Expert Bean, at pp. 7-8.

However, in producing the Laptop and Acronis images, the FBI materially deviated from standard forensic procedures. Specifically, the FBI failed in the following regards:

1) There is no documentation concerning the forensic imaging process;

2) There is no documentation concerning the devices that were imaged (*i.e.*, pictures, logs, worksheets, etc.);

---

[8]CMOS (Complementary Metal Oxide Semiconductor) memory is the computer function that controls the date, time, and other information relating to basic system settings.

[9]BIOS (Basic Input Output System) is "[t]he set of user–independent computer instructions stored in a computer's ROM [Read Only Memory], that is immediately available to the computer when the computer is turned on. BIOS information provides the code necessary to control the keyboard, display screen, disc drives and computer communication ports in addition to handling certain miscellaneous functions." Shira A. Scheindlin & Daniel J. Capra, *Electronic Discovery and Digital Evidence* at 659–60 (West 2009).

3) There is no documentation of any CMOS or BIOS data from the devices that should have been documented at the time of the imaging;

4) There is no documentation of any of the hard drive information that was imaged (*i.e.*, make, model, serial number, size, jumper settings); and

5) There is no documentation as to what equipment the FBI used to make the image (hardware and software).

*See* Declaration of Forensic Computer Expert Bean, at pp. 8-9. While it is difficult to assess the ultimate impact of these deviations from recognized forensic computer examination protocol, there is no doubt that these deviations from accepted practice seriously undermine confidence in the validity of the Wu Laptop and Acronis images.[10]

In addition, although Wu did not arrive in the United States until October 17, 2006 - and despite the fact that the Acronis backup file is dated the same day - the images produced by the FBI bear creation dates prior to October 17, 2006. *See* Declaration of Forensic Computer Expert Bean, at pp. 6-7.[11] The FBI did not have possession of either the USB external hard drive holding the Acronis backup file or the Wu laptop until October 20, 2006. These unexplained dating discrepancies further undermine the reliability of the Wu Laptop and Acronis images.

[10]In light of this issue, Defendant has also submitted a separate pleading seeking discovery pursuant to Fed.R.Crim.P. 16(a)(1)(E)(i) or the issuance of a Fed.R.Crim.P. 17(c) subpoena for discovery of the FBI's forensic policies and procedures as well as guidelines associated with any applicable certificates of accreditation that may shed light on these deficiencies.

[11]The FBI's forensic image of the Acronis backup file is dated October 3, 2006, and the FBI's Wu Laptop image is dated October 5, 2006.

**C. The FBI's Wu Laptop Image Contains At Least 1,000 Files That Were Accessed, Manipulated, Or Installed After The Acronis Backup File Was Created**.

The Wu Laptop image contains over 1,000 files that appear to have been accessed, altered or added subsequent to the date of the Acronis backup file made by Hansen. *See* Declaration of Forensic Computer Expert Bean, at pp.6-7. In other words, although the government's forensic image of the Wu laptop hard drive has a creation date of October 5, 2006, it contains over 1,000 files that appear to have been accessed or manipulated on dates ranging between October 18 and October 20, 2006 – the time period during which Hansen and Hoffman had exclusive access to and control over the Wu laptop computer. While the date of creation accompanying the FBI's Wu Laptop images may be attributable to simple carelessness (if not disregard for proper forensic safeguards), the presence of the additional 1,000 files exacerbates the already dubious circumstances surrounding the chain of custody over Wu's computer. Not only does the presence of the 1,000 files raise serious concerns about the trustworthiness of the contents of the Wu Laptop image, it also suggests that some form of tampering or manipulation of the Wu hard drive occurred while it was in the possession of Hansen and/or Hoffman. Consequently, the integrity of the Acronis backup file is also implicated.

**D. Installation Of The Acronis Software By Hansen Would Have Overwritten Any Deleted Data On The Wu Laptop Computer, Thereby Removing Traces Of Impropriety By Hansen And Hoffman**.

As a general matter, information deleted from a computer is still available for a limited period of time. However, over time this "deleted" information becomes inaccessible as new information is added to the hard drive. A computer hard drive possesses a finite amount of new space to store information. Over time, that space is filled by the information and programs added

to the computer. When items are deleted, the space they formerly occupied is re-allocated to a pool ready to be filled with new information. But, only when new information is actually saved to that formerly allocated space, does the "deleted" information become completely inaccessible. *See* Scott A. Carlson & Patrick E. Zeller, *E-Discovery and Trade Secrets Law: Limitations on Discovery*, 2 No. 4 Landsl. 5, 5 (March/April 2010) ("'[D]eleted' files exist because of the manner in which computer operating systems store files. When files are deleted by a user, they are not removed from the hard drive; instead, the operating system simply no longer keeps track of them. Over time, these deleted files may be overwritten completely or in part because of the addition of new files and continued use of the computer involved."); *see also Antioch Co. v. Scrapbook Borders, Inc.*, 210 F.R.D. 645, 651–52 (D. Minn. 2002) (citing favorably testimony that "data which is deleted from a computer is retained on the hard drive, but is constantly being overwritten by new data, through the normal use of the computer equipment); *United States v. Crist*, 627 F.Supp. 2d 575, 578 (M.D. Pa. 2008) (summarizing proper forensic procedures, and noting that "deleted" files may be recovered only "as long as those files have not been written over").

Thus, additional concerns are raised by Hansen's installation of the Acronis imaging software on Wu's laptop computer. To illustrate, consider the potential impact of that installation on one of the key issues in this case. The dates of creation of all documents found on the Wu Laptop are pivotal to the determination of who is the source of certain data and when that data was acquired. Data creation dates deleted contemporaneously with Hansen and Hoffman's possession of the Wu computer would be overwritten by the subsequent installation of Acronis software. Ostensibly, Hansen and Hoffman could have uploaded incriminating information onto Wu's computer, altered the dates associated with that information's uploading, installed Acronis to overwrite the data

associated with that change, and then made a selective digital image of the hard drive to turn over to the FBI. While such a conclusion may appear speculative, the animosity and acrimony that has characterized the actions of Hoffman and others toward Mr. Khoo, Wu, Emerson and Soutavong in this case provides substantial support for the possible occurrence of such a scenario. These concerns are more serious given the fact that, in addition to the Acronis software, both Hansen's creation of the "private" desktop folder and Hoffman's creation of the "QQ" desktop folder would have similarly displaced a very significant amount of information stored on unallocated space.

In sum, a seriously tainted chain of custody and exacerbating circumstances undermine the reliability of the Wu Laptop and Acronis images as being in any way trustworthy reproductions of the data contents and configuration of the Wu laptop as it existed before it was seized by Hoffman. Rule 901 requires more than *ipse dixit* guarantees by the proponent of evidence that the evidence is what it purports to be - especially where the opposing party raises legitimate and substantiated arguments undermining authenticity. Unless the government can advance a reliable basis for establishing that the Laptop and/or Acronis images accurately reflect the contents of the original Wu laptop hard drive, this Court should exclude them from evidence pursuant to Rule 901.

## POINT IV

## THE ACRONIS AND FBI WU LAPTOP IMAGES ARE ALSO SUBJECT TO EXCLUSION IN ACCORDANCE WITH THE "BEST EVIDENCE RULE."

Federal Rule of Evidence 1002 provides that "[t]o prove the content of a writing, recording, or photograph, the original writing, recording, or photograph is required, except as otherwise provided in these rules or by Act of Congress." Notably, both the Wu Laptop and the Acronis images are reproductions of "writings" on the original Wu laptop computer hard drive. *See* F.R.E.

1001(1) ("'Writings' and 'recordings' consist of letters, words, or numbers, *or their equivalent*, set down by handwriting, typewriting, printing, photostating, photographing, magnetic impulse, mechanical or electronic recording, or other form of data compilation.") (emphasis added); F.R.E. 1001(4) ("A 'duplicate' is a counterpart produced by the same impression as the original . . . or electronic re-recording . . . or by other equivalent techniques which accurately reproduce the original."). As the Advisory Committee notes, and the definitions reflect, "the considerations underlying the rule dictate its expansion to include computers." F.R.E. 1001, Advisory Committee Notes to 1972 Proposed Rules.

### A. The Government Cannot Demonstrate That Either The Wu Laptop Image Or The Acronis Image Is A Duplicate Because They Are Not The Product Of "Techniques Which Accurately Reproduce The Original."

Rule 1001 places a burden on the proponent of duplications to prove that they are an accurate portrayal of the original. F.R.E. 1001(4). While requiring a direct molecular-level comparison between the duplicate and the original would contravene the underlying purpose of the rule, at the very least the proponent of a duplicate is required to establish that a reliable and recognized method of duplication was employed. *See* 2 *McCormick on Evidence*, *supra*, at 89–90 (Writings, recordings, and photographs "exhibit a fineness of detail lacking in chattels generally; this detail will often be of critical importance; and prevention of loss of this fine detail through mistransmission is a basic policy objective of the rule requiring production of originals.").

Accordingly, Rule 1001(4) only confers the special status of "duplicate" on copies "produced by methods possessing an accuracy which virtually eliminates the possibility of error." F.R.E. 1001, Advisory Committee Notes to the 1972 Proposed Rules. Importantly, the rough converse of this definition of "duplicate" is that "[c]opies subsequently produced manually...are not within the

definition." *Id*. The Acronis backup file created by Hansen (now preserved as the Acronis image) is far more akin to an inadmissible manual reproduction of the Wu laptop hard drive than a presumptively accurate mirror image.

**1. The Acronis Imaging Software Used By Hansen Does Not Automatically Create Mirror Image Copies Of Computer Hard Drives, And Is Thus Subject To Manipulation And Selective Copying**.

Hansen used an archival imaging tool to produce selective digital images. Quite simply, the Acronis software is unfit to produce "copies" for forensic purposes. Highlighting the shortcomings of Acronis is the distinction between archival imaging tools, such as the Acronis software, and investigative forensic imaging tools, such as Forensic Tool Kit (FTK). Investigative forensic software produces exact copies of the physical image of the hard drive.[12] By comparison, the archival software produces only a copy of that data selectively chosen by the operator. The difference is dramatic. A person utilizing investigative software has little or no control over the contents that are ultimately imaged, while a person utilizing archival software retains unfettered ability to manipulate the data produced. *See Digital Evidence and Computer Crime*, *supra*, at 226 ("A bitstream [a.k.a. forensic image, exact duplicate copy] duplicates everything in a cluster, including anything that is in the slack space and other areas of the disk outside of the file system's reach, whereas other methods of copying a file only duplicate the file and leave the slack space

[12]*See E–Discovery and Trade Secrets Law*, 2 No. 4 Landsl. at 5: Noting that "mirror image" copying is the most common method of forensic imaging and that "these forensic copies cover the entire contents of the hard drive, including, generally: (1) the files created by a user (word processing files, e-mail, spreadsheets, etc.); (2) files that run the various applications, programs, and operating system on the computer, including log files, Internet history, etc.; and (3) information related to files that have been deleted, including the potential recovery of partial or complete copies of deleted files."

behind. Therefore, digital evidence will be lost if a bitstream copy is not made."); *see also* Declaration of Forensic Computer Expert Bean, at pp. 4.

In *Gates Rubber Co. v. Bando Chemicals Indus., Ltd.*, the court found "file-by-file" imaging far inferior to the industry standard of "mirror image copying" because it posed an unjustifiable risk of data manipulation and information loss. 167 F.R.D. 90, 112–113 (D. Colo. 1996) (issuing discovery sanctions due, in part, to the decision to utilize file-by-file instead of mirror imaging). *Gates Rubber Co.* reflects the main advantage of mirror imaging: "it ensures [that people] cannot tamper with the evidence, at least without detection." EnCase Legal Journal, *The Practitioner's Guide to Legal Issues Related to Digital Investigations and Electronic Discovery* §8.1 (Sept. 2009 ed.). The reduction in the risk of tampering associated with modern duplication methods has been advanced as the primary justification for the liberal treatment of "duplicates" under F.R.E. 1003. *See 2 McCormick on Evidence*, *supra*, at 98–100 (explaining that "duplicates" are accepted in lieu of originals largely because they are the product of scrupulous modern copy methods). Policy considerations concerning reduction of the risk of tampering have shaped the definitional scope of the term "duplicates" as such is used in Rule 1001(4), and those same policy consideration frame the center of controversy in this case.

**2. The Process Of Installing Acronis Imaging Software Deletes Underlying Data, Therefore The Acronis And Wu Laptop Images That Were Produced After Hansen Installed Acronis Cannot Be Said To Be Accurate Duplications Of The Original Wu Hard Drive**.

Similarly problematic, Hansen did not utilize an Acronis imaging software already present on Wu's computer; instead, he first installed the Acronis program in order to retrieve and copy the files ultimately reproduced on the Acronis digital image. As noted in Section II (D), *supra*, this

process not only adds new information to a computer, it also overwrites certain other information. *See Antioch Co.*, 210 F.R.D. at 651–52; *E-Discovery and Trade Secrets Law*, 2 No. 4 Landsl. at 5. Thus, Hansen's activity raises serious issues concerning the accuracy of both the Acronis and Wu Laptop images. Information loss caused by the installation of the Acronis software taints both the Acronis and Laptop digital images, rendering questionable their status as "duplicates" of the original Wu Laptop hard drive. *See* Declaration of Forensic Computer Expert Bean, at pp. 4-5. This concern is exponentially increased given that Hansen, Hoffman and/or the FBI made multiple attempts to either load software on, or generate copies of, the Wu Laptop hard drive, and as well accessed and installed several executable files onto Wu's computer, not simply Acronis. *See* Declaration of Forensic Computer Expert Bean, at pp. 5-7.

**3. The FBI Did Not Follow Proper Forensic Procedures In Creating The Laptop Image Of Wu's Hard Drive, And Therefore The Government Cannot Prove That The Laptop Image Is The Result Of An Accurate And Reliable Imaging Methodology**.

As noted in Section II(B), *supra*, certain specific forensic procedures must be followed in order to ensure that a digital image is the product of a reliable and accurate imaging process. To date, Mr. Khoo has not received any supporting documentation as to the forensic imaging procedure actually employed by SA Brillhart in creating the Wu Laptop and Acronis images. The questionable data-creation dates indicate that proper forensic procedures were not followed. Because there is no documentation indicating what procedures were utilized by SA Brillhart, and because no explanation has yet been forthcoming with respect to the data-creation dates and other deficiencies hereinbefore described, the status of Wu Laptop image as being a reliable copy of the Wu hard drive is clearly in question.

**B. Even If The Acronis And Laptop Images Qualify As "Duplicates," The Exceptions To Admissibility Of Duplicates In Lieu Of Originals Grounded In Rule 1003 Bar Their Admission**.

Even if this Court concludes that the Acronis and/or Laptop images qualify as a "duplicate," the government can only admit these images if they are not subject to the exceptions set forth in F.R.E. 1003. Rule 1003 provides that "[a] duplicate is admissible to the same extent as an original unless (1) a genuine question is raised as to the authenticity of the original or (2) in the circumstances it would be unfair to admit the duplicate in lieu of the original."

**1. "A Genuine Question" Has Been Raised As To The Contents Of The Wu Laptop Hard Drive, Prior To It's Seizure By Hansen And Hoffman**.

In construing the scope of Rule 1003, this Court must be sensitive to the Congressional "expectation that the courts would be liberal in deciding that a 'genuine question is raised as to the authenticity of the original.'" F.R.E. 1003, Advisory Committee Notes to the 1974 Enactment (citing H.R. No. 93–650 (Nov. 15, 1973), reprinted in 1974 U.S.C.A.A.N. 7051, 7090). Applying this principle, neither the Acronis nor the Laptop image is admissible because there is a genuine question as to the authenticity of the contents of the original Wu computer hard drive.

A "genuine question" may arise under a variety of situations, but two are particularly relevant in this case. First, a genuine question arises when alterations obscure precisely what the content of the original was. *See SEC v. Hughes Capital Corp.*, 124 F.3d 449, 456 (3d Cir. 1997) (photocopies of check stubs were properly excluded, since stubs had been altered before photocopying and the party responsible for the alterations cannot identify exactly what was altered). Here, the presence of 1,000 accessed and/or altered files indicates alterations prior to the production of the Wu Laptop image. Second, a genuine question arises where two purported copies of the same original are

materially different, and the original is not available to verify which is the more accurate reproduction. *See Opals on Ice Lingerie v. Body Lines, Inc.*, 320 F.3d 362, 371 (2d Cir. 2003) (copies inadmissible where both parties produced different copies and neither party could produce original). The variations between the Acronis and the Laptop images are drastic – the Wu Laptop image contains 1,000 files, the source of which are uncertain. Even if the Wu Laptop computer hard drive is still available, it is likely that its data content and configuration have been damaged during the process of undergoing multiple rounds of forensic imaging. *See Electronic Discovery and Digital Evidence*, *supra*, at 65 ("forensic examinations often involve destructive testing"). Declaration of Forensic Computer Expert Bean, at p. 5.

In addition to the indications of possible data manipulation and the problem of inconsistent "copies," several other concerns are present: (1) Basic safeguards secured by proper forensic procedures have been violated; (2) A party with a motive, opportunity, and ability to manipulate the contents of the Wu Laptop maintained possession of it for several days under circumstances suggesting impropriety; and (3) The government cannot establish a direct link between the images in its possession and the data content and configuration of the original Wu Laptop computer hard drive as of the date of its seizure by Hoffman and Hansen. Given the totality of these circumstances, a genuine question exists as to the contents of the original Wu Laptop computer hard drive that cannot be answered by reference to the duplicates Laptop and Acronis images. Therefore, under Rules 1002 and 1003, those images are inadmissible to prove the contents of the original Wu Laptop computer hard drive. *See, e.g., United States v. Haddock*, 956 F.2d 1534, 1545–46 (10th Cir. 1992), abrogated on other grounds by *United States v. Wells*, 519 U.S. 482 (1997) ("despite our age of technology, a trial court must still be wary of admitting duplicates where the circumstances

surrounding the execution of the writing present a substantial possibility of fraud.") (citations omitted); *see also* 6 Jack B. Weinstein & Margaret A. Berger, *Weinstein's Federal Evidence* at 1003–10 (2d ed. 2010) ("If the circumstances surrounding the execution of the writing present a substantial possibility of fraud, the reliability of a duplicate as an accurate reproduction will be impaired and the court would be authorized to insist on the original if the opponent demands it.").

**2. Under The Circumstances Of This Case, It Would Be Unfair To Allow Introduction Of The Laptop And Acronis Images Because Deletions Caused By Installation Of The Acronis Software May Have Destroyed Impeachment Material Central To Proof That The Data Content Of The Laptop Was Manipulated**.

The ability to challenge evidence of guilt with all relevant information is a jealously guarded right under the United States Constitution. *See, e.g., United States v. Crawford*, 541 U.S. 36, 61 (2004) ("Where testimonial statements are involved, we do not think the Framers meant to leave the Sixth Amendment's protection to the vagaries of the rules of evidence, much less to amorphous notions of 'reliability.'"); *United States v. Giglio*, 405 U.S. 150 (1972) (all material information relevant to impeachment must be disclosed by prosecution); *United States v. Crawford*, 541 U.S. 36, 61 (2004) ("Where testimonial statements are involved, we do not think the Framers meant to leave the Sixth Amendment's protection to the vagaries of the rules of evidence, much less to amorphous notions of 'reliability.'"); *United States v. Stever*, No. 09–30004, 2010 WL 1757926 at * 6 (9th Cir. May 4, 2010) (quoting *Holmes v. South Carolina*, 547 U.S. 319, 324 (2006) (Whether grounded in the Fifth or Sixth Amendment, "the Constitution guarantees criminal defendants a meaningful opportunity to present a complete defense.") (citations omitted).

In recognition of these constitutional principles, Rule 1003 provides that a duplicate is inadmissible if "it would be unfair to admit the duplicate in lieu of the original." Admission of either

the Acronis or Laptop image would be unfair under the circumstances of this case. Allowing the government to choose, or forcing Mr. Khoo to choose, which of the alleged "duplicates" actually constitutes an accurate portrayal of the original Wu Laptop computer hard drive would substantially impair his right to be confronted with authentic and accurate evidence. *See United States v. Stephenson*, 121 F.Supp. 274, 279 (D. D.C. 1954) (excluding all of a multiplicity of differing tape recordings, despite the possibility of redaction, because forcing the defendant to choose to be confronted with compromised evidence is impermissible); *see also Lozano v. Ashcroft*, 258 F.3d 1160, 1166 & n. 5 (10th Cir. 2001) (citing *Amoco Production Co. v. United States*, 619 F.2d 1383, 1391 (10th Cir. 1980)) (exclusion of duplicate appropriate where its incompleteness would undermine the ability to accurately challenge the contents of the original).

When inconsistencies between various duplicates are shown to exist, the proponent of the evidence must establish some principled and accurate method to establish which copy is actually what it purports to be – a duplicate of the original. Arbitrarily allowing admission of one, or both, of the Wu laptop images as "duplicates," while ignoring the presence of the other, would ignore substantial evidentiary concerns to the unilateral detriment of Mr, Khoo and the other charged defendant(s). Due process of law does not countenance so capricious a result, and neither does Rule 1003.

## CONCLUSION

Several federal rules of evidence bar admission of the Laptop and Acronis hard drive images in this case. First, Rule 901 prevents the government from offering either the Laptop or Acronis hard drive images because they cannot establish a sufficient connection between the contents on those images and Mr. Wu. Second, the Laptop and Acronis hard drive images do not qualify as

"duplicates" of the original Wu hard drive, and, even if they did, questions as to authenticity and the unfairness involved in admitting them require their exclusion pursuant to Rule 1003. Accordingly, Mr. Khoo moves this Court to exclude the Acronis and Wu Laptop images from admission into evidence.

Respectfully submitted this May 28, 2010.

*/s/ Christopher J. Schatz*
Christopher J. Schatz
Attorney for Defendant Hock Chee Khoo

Greg Rapkoch
Legal Research Assistant